Transportation Worker Identification Credential (TWIC) Qualified Technology List (QTL) Program

Portable Physical Access Control Reader Approval Procedures

May 23, 2012

Version 1.1

Department of Homeland Security
Transportation Security Administration
Office of Security Policy and Industry Engagement
601 S. 12th Street
Arlington, VA 22202

Revision History

Version / Date	Edits / Changes
Sept 13, 2010; v0.1	Initial Internal Version (based on v0.2 of the TWIC Fixed Reader AP)
Oct 15, 2010; v0.2	Updates based on comments from NIST
Oct 19, 2010; v0.3	Updates to synchronize with the test procedure
Oct 26, 2010; v0.4	Updates based on comments from TSA
Dec 20, 2010; v0.5	Updates based on DTR v0.6
Feb 08, 2011; v0.6	Replaced "Hotlist" with "Canceled Card List"
Apr 19, 2012; v0.7	Updates based on draft technical bulletin clarification of specification and other editorial changes
Apr 20, 2012; v1.0-draft-20120420	Promote to version 1.0 for NVLAP Lab release
Apr 20, 2012; v1.0-draft-20120511	Minor updates
May 21, 2012; v1.1	Final TSA comments for NVLAP lab release
May 23, 2012; v1.1	TSA released

TABLE OF CONTENTS

LIST OF TABLES

TWIC QTL Portable Physical Access Control Reader Approval Procedures

1 Introduction

1.1 Background

The United States Congress mandated the Transportation Worker Identification Credential (TWIC) in the Maritime Transportation Security Act of 2002 (MTSA) as amended by the Security and Accountability for Every Port Act of 2006 (SAFE Port Act). The mission of the TWIC Program is to design and field a tamper resistant credential (referred to as a TWIC card) for all maritime workers requiring unescorted physical access to secure areas of the nation's port facilities, outer continental shelf facilities, and vessels regulated under the MTSA, and all U.S. Coast Guard credentialed merchant mariners. The TWIC program is administered by the Department of Homeland Security (DHS) with joint management responsibility shared by the Transportation Security Administration (TSA) and the U.S. Coast Guard. TSA is responsible for enrollment, identity vetting and credential issuance. The Coast Guard is responsible for enforcement, access control requirements and regulations.

The TWIC card is subject to visual inspection at points of entry or can be automatically read and validated by reader devices which have been deployed by maritime operators. The TWIC Reader Hardware and Card Application Specification (hereafter, referred to as the TWIC Specification) is a document issued by the Transportation Security Administration (TSA) which describes the behavior of the TWIC card application, card interface, as well as the reader hardware performance and technical requirements. The TWIC Specification addresses both fixed and portable reader devices.

The Transportation Security Administration (TSA) working with the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and other federal agencies has established a process and program to test and qualify TWIC reader products that read, verify, and authenticate the TWIC cards used in the TWIC Program. Products that are deemed to be compliant with the TWIC Specification will be placed on a list referred to as the TWIC Reader Qualified Technology List (QTL) which can be used by owners and operators of regulated maritime facilities and vessels to assist in their TWIC reader purchasing decisions.

The TSA TWIC Program Management Office operating under the TSA Office of Security Policy and Industry Engagement (OSPIE) has established the QTL program to provide an on-going process of TWIC reader qualification by independent laboratories accredited by NIST under the National Voluntary Laboratory Accreditation Program (NVLAP). The initial focus of the QTL effort is to establish NVLAP accredited test laboratories capable of assessing the conformance of fixed and portable TWIC readers with the TWIC Reader Hardware and Card Application specification.

1.2 Purpose and Scope

This document (referred to as the Approval Procedure) provides details on the requirements that a Portable TWIC Reader must meet to be included on the Qualified Technology List (QTL).

Per the TWIC specification, a Portable TWIC Reader is defined as a *handheld TWIC reader that may be used for portable, spot-check identity verification.*
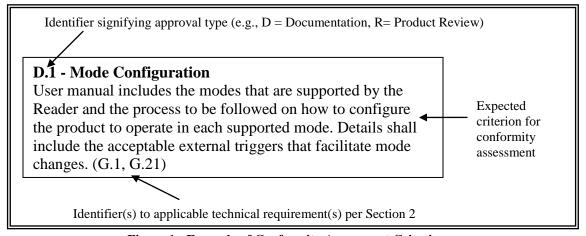
This approval procedure provides details on the application submission requirements that an Applicant shall provide in order for their TWIC Portable Reader to be included for listing on the Qualified Technology List (QTL).

1.3 Understanding the Approval Procedure

Applicants that are interested in developing Portable TWIC Reader products conformant to the TWIC specification need to reference this approval procedure to determine: (i) the requirements that apply to a Portable TWIC Reader under the TWIC specification, and (ii) the information (documentation, artifacts, test results etc.) to be submitted to the QTL Program to demonstrate conformity of the product to these requirements.

Section 2 of this document describes the product review activities or various types of documentation (e.g., test results, Applicant documentation etc.) that needs to be submitted along with the product application. Each required application package artifact is assigned an identifier that is associated with the type of approval mechanism. For example, product reviews are prefixed with an identifier of "R", while documentation submission criteria are prefixed with a "D".

Figure 1 provides an example of the applicant documentation content that is required to demonstrate the capability of the product to configure authentication modes.

Identifier signifying approval type (e.g., D = Documentation, R= Product Review)

D.1 - Mode Configuration
User manual includes the modes that are supported by the Reader and the process to be followed on how to configure the product to operate in each supported mode. Details shall include the acceptable external triggers that facilitate mode changes. (G.1, G.21)

Expected criterion for conformity assessment

Identifier(s) to applicable technical requirement(s) per Section 2

Figure 1 - Example of Conformity Assessment Criterion

Portable TWIC Reader Requirements
In general, technical requirements for TWIC Readers are classified into the following categories:

- **Mandatory Requirements** – These requirements apply to all readers. Conformance shall be demonstrated in order to get listed on the QTL.

- **Conditional Requirements** – These requirements do not apply to all readers. Conformance shall be demonstrated in order to get listed on the QTL only if the reader claims to have certain characteristics (e.g. can operate outdoors) or support certain functionality (e.g. biometric capability)

- **Optional Features** – Optional features are those that are recommended by the specification, but not mandated. Readers may implement such features however it is not compulsory for these to be implemented in order to be listed on the QTL.

The following sub-sections identify the mandatory and conditional requirements, as well as the optional features that apply to a Portable TWIC Reader under the TWIC specification. Along with each requirement is an approval mechanism which identifies the method that is used to determine conformity. Please note that a requirement may have multiple approval mechanisms. Section 3 provides the definition and details of each type of approval mechanism.

1.4 General

This section identifies all mandatory requirements and optional features that apply to a Portable TWIC Reader regardless of supported modes, interfaces or location.

1.4.1   Mandatory

Every reader submitted for listing on the QTL shall meet all of the requirements listed in Table - 1.

Requirement ID	Requirement Description	Approval Mechanism
G.1	TWIC Readers shall support configuration of one or more authentication modes per Table 4.1, TWIC Identification and Authentication Modes.	Applicant Documentation (D.1)
G.2	TWIC readers shall operate within a range of 8-48 VDC.	Applicant Documentation (D.3)
G.3	Where necessary to operate from line voltage, a power supply approved for use with a TWIC reader shall be provided.	Product Review (R.1)

TWIC QTL Portable Physical Access Control Reader Approval Procedures

Requirement ID	Requirement Description	Approval Mechanism
G.4	All TWIC readers shall not exceed a 2.0 Amperes current requirement.	Applicant Documentation (D.3)
G.5	All TWIC readers shall provide reverse voltage protection.	Applicant Documentation (D.3)
G.6	All TWIC readers shall be FCC certified.	Electrical Testing (E.1)
G.7	All TWIC readers shall return automatically to normal operation after a loss of power event.	Functional Testing
G.8	Intentionally left blank.	
G.9	All TWIC readers shall not possess sharp corners or edges that may puncture, cut, or tear the skin or clothing or otherwise cause bodily injury.	Product Review (R.2)
G.10	All TWIC readers shall not possess external wires, connectors, or cables other than the power cable, data cable and the optional TWIC Privacy Key reading sub-assembly (i.e. magnetic stripe reader).	Product Review (R.2)
G.11	All TWIC readers shall not possess loose coverings and cowlings.	Product Review (R.2)
G.12	Cryptographic algorithms within the reader are implemented correctly.	Product Review (R.5)
G.13	Visual indicators for all TWIC Readers shall be visible in daylight.	Product Review (R.3)
G.14	All TWIC readers shall provide a means to create a time-stamped log of operations for use in assessing exception conditions such as fingerprint rejections.	Applicant Documentation (D.6) Functional Testing
G.15	All TWIC readers shall be designed to yield a Mean Time Between Failure (MTBF) of 25,000 hours or greater.	Reliability Testing (RE.1)
G.16	All TWIC readers shall include technical manuals covering installation, operation and maintenance.	Product Review (R.4)
G.17	All TWIC Readers shall explicitly select the TWIC Application while performing the user authentication.	Functional Testing

TWIC QTL Portable Physical Access Control Reader Approval Procedures

Requirement ID	Requirement Description	Approval Mechanism
G.18	In TWIC readers using the TWIC card, the SELECT "AID" APDU command shall always ask for a partial TWIC AID and analyze the information returned from a TWIC card when the SELECT APDU command is successful.	Functional Testing
G.19	All TWIC readers shall require that a TWIC card, once read, shall be removed from the RF field for at least one second before attempting to read any new contactless card	Functional Testing
G.20	A TWIC reader (or panel, with bi-directional wiring) shall be locally configurable with the X.509 certificate containing the public key for all currently active Certificate Authorities (CAs) that are trusted for issuance of TWIC Certificates.	Functional Testing
G.21	TWIC readers that support multi-mode operation shall be able to accept external triggers for the mode change.	Applicant Documentation (D.1)
G.22	The Operational TWIC Card AID (A0 00 00 03 67 20 00 00 01 01 01) shall be recognized.	Functional Testing
G.23	A TWIC reader shall verify if the TWIC reader supports the release edition (or test mode) returned by the TWIC card.	Applicant Documentation (D.7)
G.24	The contactless smart card TWIC reader component shall conform to the ISO/IEC 14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201-1.	Applicant Documentation (D.8)
G.25	TWIC readers shall have a maximum contactless smart card read range of 10cm.	Functional Testing
G.26	Contactless enabled TWIC readers shall be able to communicate with a contactless card at 106kbit/s, 212kbit/s or 424kbit/s.	Applicant Documentation (D.8)
G.27	A TWIC Reader shall reject all of the presented cards, if two or more contactless smart cards are presented at the same time in a TWIC reader's contactless field.	Functional Testing
G.28	All data shall be retrieved from the TWIC card application for all authentication modes except for operations involving Active Card Authentication.	Functional Testing
G.29	The Test TWIC Card AID (A0 00 00 03 67 20 00 00 01 81 01) shall be recognized	Functional Testing

TWIC QTL Portable Physical Access Control Reader Approval Procedures

Requirement ID	Requirement Description	Approval Mechanism
G.30	The key required to decipher the reference biometric template of the user, called the TWIC Privacy Key (TPK), shall be obtained from one of several sources. These sources include the magnetic stripe encoded on each TWIC card, the TWIC card memory (but only accessible through the contact interface) or from the physical access control system where the TPK has been registered.	Functional Testing
G.31	TWIC readers shall support the V1.0 and V2.0 marked TWIC cards in all supported modes of operation.	Functional Testing
G.32	The TWIC reader log of operations shall include the current date as year, month and day and the current time as hours, minutes and seconds.	Functional Testing
G.33	The TWIC reader log of operations shall include the card FASC-N of each TWIC card presented, the operation performed using the card (reader mode) and the status of the operation (success or failure) with an indication of the reason for any failures.	Functional Testing
G.34	TWIC readers shall provide a means to export the TWIC reader log of operations in human-readable form in the English language.	Functional Testing

Table 1 - Mandatory Requirements for Portable TWIC Readers

1.4.2   Optional

A reader submitted for listing on the QTL may implement the features listed in Table -2. However, it is not required that the reader implement these features to be listed on the QTL.

Requirement ID	Requirement Description	Approval Mechanism
GO.1	All TWIC Readers should provide a mechanism that assures that only authorized/authenticated firmware/software updates are permitted.	Applicant Documentation (D.9)

Requirement ID	Requirement Description	Approval Mechanism
GO.2	A TWIC Reader may configure itself in a diagnostic mode for the purpose of testing/diagnostics with test TWIC Cards	Applicant Documentation (D.10)
GO.3	All TWIC reader corners and edges should have at least a 1mm exposed radius of curvature.	Product Review (R.8)
GO.4	All TWIC readers should clearly and continuously display power status (on, ready or out of service).	Product Review (R.9)
GO.5	The interface between the TWIC card and a TWIC reader may be via the contact or the contactless interface.	Applicant Documentation (D.5), Functional Testing

Table 2 – Optional Features for Portable TWIC Readers

1.5 Portable Readers

The following requirements apply to portable readers.

1.5.1   Mandatory

Every portable reader submitted for listing on the QTL shall meet all of the requirements listed in the Table - 3.

Requirement ID	Requirement Description	Approval Mechanism
P.1	A portable TWIC reader shall be capable of confirming whether a TWIC card has been revoked by downloading and using a TWIC Canceled Card List.	Applicant Documentation (D.2), Functional Testing
P.2	Portable TWIC readers shall have a display suitable for user interaction.	Product Review (R.3)
P.3	Portable TWIC readers shall be able to display the current battery level.	Product Review (R.6)
P.4	Portable TWIC readers shall have a real time clock.	Applicant Documentation (D.5), Product Review (R.7)

TWIC QTL Portable Physical Access Control Reader Approval Procedures

Requirement ID	Requirement Description	Approval Mechanism
P.5	Portable TWIC readers that support connection to a PACS to operate access control devices shall comply with UL 294, Standard for Safety of Access Control System Units, or internationally recognized equivalent.	Applicant Documentation (D.14)
P.6	Portable TWIC readers shall support expiration checking.	Applicant Documentation (D.13), Functional Testing

Table 3 - Mandatory Requirements for Portable TWIC Readers

1.5.2   Optional

A reader submitted for listing on the QTL may implement the features listed in Table - 4. However, it is not required that the reader implement these features to be listed on the QTL.

Requirement ID	Requirement Description	Approval Mechanism
PO.1	A portable TWIC reader may support a Certificate Revocation List (CRL) subject to availability of a network connection.	Functional Testing
PO.2	Portable TWIC readers may use a touch screen or other suitable means for user input/control.	Product Review (R.10)
PO.3	If a portable TWIC reader has only a contactless card read capability, the portable TWIC reader shall also have a magnetic stripe reader in order to access the TWIC Privacy Key.	Product Review (R.11)
PO.4	Portable TWIC readers that support a wireless interface to provide direct access to a PACS shall have the following security attributes: • confidentiality (session key) • active authentication of the TWIC reader or, the operator using the TWIC reader.	Applicant Documentation (D.11)
PO.5	Portable TWIC readers should have a hibernation mode for protection against data loss.	Applicant Documentation (D.12)
PO.6	A portable verification reader may also have the ability to communicate with an external access control system to control a door, gate, etc. via a Wiegand or other output format.	Applicant Documentation (D.15), Functional Testing

Table 4 - Optional Features for Portable TWIC Readers

1.6 Outdoor Readers (Conditional Requirements)

The following conditional requirements apply to readers that operate outdoors.

1.6.1   Mandatory

Every reader submitted for listing on the QTL shall meet all of the requirements listed in Table - 5.

Requirement ID	Requirement Description	Approval Mechanism
OUT.1	All TWIC readers shall conform to a NEMA 4 rating.	Environmental Testing (EN.7)
OUT.2	All TWIC readers shall be capable of operations in direct sunlight. All TWIC readers shall neither require nor be affected by ambient light sources.	Environmental Testing (EN.8)

Table 5 - Mandatory Requirements for Outdoor TWIC Readers

1.7 Readers used in Harsh Conditions (Conditional Requirements)

The following conditional requirements shall apply to readers that operate in harsh conditions.

1.7.1   Mandatory

Every reader submitted for listing on the QTL shall meet all of the requirements listed in Table - 6.

Requirement ID	Requirement Description	Approval Mechanism
PH.1	Portable TWIC readers certified for harsh conditions shall meet the MIL-STD 810F, Method 514.5 for Vibration.	Environmental Testing (EN.1)
PH.2	Portable TWIC readers certified for harsh conditions shall meet the MIL-STD 810F, Method 501.4 for High temperature (to +70°C/+158°F).	Environmental Testing (EN.2)
PH.3	Portable TWIC readers certified for harsh conditions shall meet the MIL-STD 810F, Method 502.4 for Low temperature (to -10°C/+14°F).	Environmental Testing (EN.3)
PH.4	Portable TWIC readers certified for harsh conditions shall meet the MIL-STD 810F, Method 507.4 for Humidity.	Environmental Testing (EN.4)

TWIC QTL Portable Physical Access Control Reader Approval Procedures

Requirement ID	Requirement Description	Approval Mechanism
PH.5	Portable TWIC readers certified for harsh conditions shall meet the MIL-STD 810F, Method 503.4 for Temperature shock.	Environmental Testing (EN.5)
PH.6	Portable TWIC readers certified for harsh conditions shall meet the MIL-STD 810F, Method 516.5, Procedure IV (Transit Drop Test) - 26 drops at 4 feet.	Environmental Testing (EN.6)

Table 6 - Mandatory Requirements for TWIC Readers used in Harsh Conditions

1.8 TWIC Authentication Mode Requirements (Conditional Requirements)

The conditional requirements listed within this sub-section are categorized based on the TWIC authentication modes. Readers are required to implement those requirements that apply to the mode that they support. It is not required for the reader to support all authentication modes specified by TWIC.

1.8.1   Authentication Mode 1

The following requirements apply to a reader that supports CHUID verification mode.

1.8.1.1 **Mandatory**

Every reader submitted for listing on the QTL shall meet all of the requirements listed in Table - 7.

Requirement ID	Requirement Description	Approval Mechanism
M1.1	TWIC readers may support Signed CHUID Verification	Functional Testing
M1.2	The TWIC reader verifies that the id-TWIC-content-signing object identifier is present in the card issuer's digital signature certificate for the document signer. If the id-TWIC-content-signing object identifier is not present in the card issuer's digital signature certificate for the document signer, the TWIC reader shall reject the card.	Functional Testing
M1.3	TWIC readers shall verify the CHUID signature and origin up to and including the trust anchor.	Functional Testing

TWIC QTL Portable Physical Access Control Reader Approval Procedures

M1.4	TWIC reader shall decode the FASC-N TLV record and extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential issue. The TWIC reader may transmit data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or selected elements of the FASC-N.	Functional Testing
M1.5	If a TWIC reader is configured for expiration checking using the signed CHUID, the date encoded in the signed CHUID data object is compared to the current date/time. If the date encoded in the signed CHUID data object is before the current date/time, the reader shall reject the card.	Functional Testing
M1.6	If the TWIC reader is configured to use the TWIC Cancelled Card List to check for card revocation using the signed CHUID, the TWIC reader checks to see if the FASC-N from the signed data object is listed on the latest version of the CCL accessed by the reader. If the FASC-N from the signed CHUID data object is listed on the latest version of the CCL accessed by the reader, the TWIC reader shall reject the presented card.	Functional Testing
M1.7	When configured for unsigned CHUID signature verification using the Security Data Object, the TWIC reader shall verify the signature and origin of the unsigned CHUID, up to and including the trust anchor using the Security Data Object.	Functional Testing
M1.8	When configured for unsigned CHUID signature verification using the Security Data Object, if the id-TWIC-content-signing object identifier is not present in the card issuer's digital signature certificate for the document signer of the Security Data Object, the TWIC reader shall reject the card.	Functional Testing

TWIC QTL Portable Physical Access Control Reader Approval Procedures

M1.9	3) If a TWIC reader is configured for expiration checking using the unsigned CHUID, the date encoded in the unsigned CHUID data object is compared to the current date/time. If the date encoded in the unsigned CHUID data object is before the current date/time, the reader shall reject the card.	Functional Testing
M1.10	5) If the TWIC reader is configured to use the TWIC Cancelled Card List to check for card revocation using the unsigned CHUID, the TWIC reader checks to see if the FASC-N from the unsigned CHUID data object is listed on the latest version of the CCL accessed by the reader. If the FASC-N from the unsigned CHUID data object is listed on the latest version of the CCL accessed by the reader, the TWIC reader shall reject the presented card.	Functional Testing

Table 7 - Mandatory Requirements for TWIC Readers supporting Authentication Mode 1

1.8.1.2 **Optional**

A reader submitted for listing on the QTL may implement the features listed in Table - 8. However, it is not required that the reader implement these features to be listed on the QTL.

Requirement ID	Requirement Description	Approval Mechanism
M1O.1	Alternatively, a TWIC reader may perform Unsigned CHUID signature verification using the Security Data Object.	Functional Testing
M1O.2	The TWIC reader may support use of the unsigned CHUID without signature verification for use in cases where the CHUID signature has been previously verified by and registered in the PACS.	Functional Testing

Table 8 - Optional Requirements for TWIC Readers supporting Authentication Mode 1

1.8.2   Authentication Mode 2

The following requirements apply to a reader that supports the Active Card Authentication mode

1.8.2.1 **Mandatory**

Every reader submitted for listing on the QTL shall meet all of the requirements listed in Table - 9.

TWIC QTL Portable Physical Access Control Reader Approval Procedures

Requirement ID	Requirement Description	Approval Mechanism
M2.1	TWIC readers may support Active Card Authentication	Functional Testing
M2.2	A TWIC reader, or the system to which the TWIC reader is connected, shall support asymmetric cryptographic operations.	Functional Testing
M2.3	The reader shall compare the "issuer" name in the Certificate against the "subject" name in each trusted issuing CA certificate stored on a TWIC reader. For each CA with a matching name, the Public Key is used to attempt to verify the signature on the token's certificate. If no matching CA certificate is found on a TWIC reader with the same name and with a Public Key that verifies the signature on the certificate, then the reader shall reject the card containing the certificate.	Functional Testing
M2.4	If a TWIC reader is configured for expiration checking using card authentication, the date encoded in the Card Authentication Certificate's "notBefore" validity date is after the current date/time, or if the Certificate's "notAfter" validity date is before the current date/time, the reader shall reject the card containing the Certificate.	Functional Testing
M2.5	The Certificate's subjectAltName extension identified as twicFASC-N (1.3.6.1.4.1.29138.6.6) name entry shall be retrieved from the certificate and used as the unique credential number (e.g. for optional transmission to a panel or back-end or to IDMS infrastructure).	Functional Testing
M2.6	The response (i.e. the card's signature) from the GENERAL AUTHENTICATE APDU command shall be verified using the Public Key from the Certificate. If verification of the response (i.e. the card's signature) from the GENERAL AUTHENTICATE APDU command fails, the TWIC reader shall reject the card.	Functional Testing

| M2.7 | If the TWIC reader is configured to use the TWIC Cancelled Card List to check for card revocation using card authentication, the TWIC reader checks to see if the FASC-N from the Card Authentication Certificate is listed on the latest version of the CCL accessible by the reader. If the FASC-N from the Card Authentication Certificate is listed on the latest version of the CCL accessible by the reader, the TWIC reader shall reject the presented card. | Functional Testing |
| M2.8 | If the TWIC reader is configured to sue the TWIC Certificate Revocation List (CRL) to check for card revocation, the TWIC reader checks to see if the Card Authentication Certificate is listed on the latest version of the CRL accessible by the reader. If the Card Authentication Certificate is listed on the latest version of the CCL accessible by the reader, the TWIC reader shall reject the presented card. | Functional Testing |

Table 9 - Mandatory Requirements for TWIC Readers supporting Authentication Mode 2

1.8.3   Authentication Mode 3

The following requirements apply to a reader that supports the CHUID Verification + Biometric User Authentication mode

1.8.3.1 **Mandatory**

Every reader submitted for listing on the QTL shall meet all of the requirements listed in Table - 10.

Requirement ID	Requirement Description	Approval Mechanism
M3.1	TWIC readers may support Signed CHUID + Biometric	Functional Testing
M3.2	The TWIC reader shall perform signed CHUID verification as defined in A.1.	Functional Testing
M3.3	The TWIC reader verifies that the digital signature on the CBEFF record was produced by an authorized document signer. This requires that the TWIC reader have a verified copy of the document signer's X.509 digital certificate. If signature verification of the CBEFF record using the public key from this verified document signing certificate fails, the TWIC reader shall reject the card.	Functional Testing

M3.4	The reader compares the FASC-N from signed CHUID with the FASC-N with the FASC-N from the CBEFF record. If the FASC-N from the signed CHUID and the FASC-N from the CBEFF record do not match, the TWIC reader shall reject the card.	Functional Testing
M3.5	The TWIC reader samples a fingerprint image from the cardholder. The TWIC reader shall convert the sampled image to a minutiae template and match the template against the fingerprint minutiae templates stored in the signed biometric data object at an appropriate level of confidence (see Section B).	Functional Testing
M3.6	If the fingerprint does not match one of the templates on the first attempt, the TWIC reader shall prompt the cardholder for subsequent attempts without requiring the TWIC card to be read again.	Functional Testing
M3.7	If the number of subsequent matching failures exceeds the reader's configurable retry counter, the TWIC reader shall reject the card.	Functional Testing

Table 10 - Mandatory Requirements for TWIC Readers supporting Authentication Mode 3

1.8.4 Authentication Mode 4

The following requirements apply to a reader that supports the CHUID Signing Certificate + Active Card Authentication + Biometric User Authentication mode.

1.8.4.1 **Mandatory**

Every reader submitted for listing on the QTL shall meet all of the requirements listed in Table - 12.

Requirement ID	Requirement Description	Approval Mechanism
M4.1	TWIC readers may support Active Card Authentication + Biometric	Functional Testing
M4.2	The TWIC reader verifies that the id-TWIC-content-signing object identifier is present in the card issuer's digital signature certificate for the document signer. If the id-TWIC-content-signing object identifier is not present in the card issuer's digital certificate for the document signer, the TWIC reader shall reject the card.	Functional Testing

TWIC QTL Portable Physical Access Control Reader Approval Procedures

M4.3	The TWIC reader shall verify the CBEFF signature and origin up to and including the trust anchor. If signature verification of the CBEFF record using the public key from the verified document signing certificate fails, the TWIC reader shall reject the card.	Functional Testing
M4.4	The reader compares the FASC-N from the Card Authentication Certificate with the FASC-N from the CBEFF record. If the FASC-N from the Card Authentication Certificate and the FASC-N from the CBEFF record do not match, the TWIC reader shall reject the card.	Functional Testing
M4.5	The TWIC reader samples a fingerprint image from the cardholder. The TWIC reader shall convert the sampled image to a minutiae template and match the template against the fingerprint minutiae templates stored in the signed biometric object at an appropriate level of confidence (see Section 8).	Functional Testing
M4.6	If the fingerprint does not match one of the templates on the first attempt, the TWIC reader shall prompt the cardholder for subsequent attempts without requiring the TWIC card to be read again.	Functional Testing
M4.7	If the number of subsequent matching failures exceeds the reader's configurable retry counter, the TWIC reader shall reject the card.	Functional Testing

Table 11 - Mandatory Requirements for TWIC Readers supporting Authentication Mode 4

1.8.5   Biometric Requirements

The following requirements apply to a reader that supports any authentication mode that involves the use of the fingerprint biometrics

1.8.5.1 **Mandatory**

Every reader submitted for listing on the QTL shall meet all of the requirements listed in Table - 12.

Requirement ID	Requirement Description	Approval Mechanism
B.1	For biometric-enabled TWIC Readers, if the number of minutiae is zero, then the TWIC Reader shall deny access.	Functional Testing

B.2	Readers shall provide an automated alert or lockout after a configurable number (facility configured) of consecutive failed biometric matching attempts	Applicant Documentation (D.16), Functional Testing
B.3	TWIC readers shall first check the number of minutiae present to determine if a 1:1 match may proceed.	Functional Testing
B.4	Biometric-enabled TWIC readers shall be able to handle 1 million touches without degradation.	Reliability Testing (RE.2)

Table 12 - Mandatory Requirements for TWIC Readers supporting Authentication Modes involving biometrics

1.8.5.2 **Optional**

A reader submitted for listing on the QTL may implement the features listed in Table - 13. However, it is not required that the reader implement these features to be listed on the QTL.

Requirement ID	Requirement Description	Approval Mechanism
BO.1	Biometric-enabled TWIC readers should provide liveness detection.	Applicant Documentation (D.18)
BO.2	Intentionally left blank.	
BO.3	Intentionally left blank.	
BO.4	All biometrically-enabled TWIC readers should provide a mechanism to adjust the security level sensitivity as required.	Applicant Documentation (D.17)
BO.5	The biometric sub-system on the TWIC Reader should provide an equal error rate (EER) of 1% (i.e. 1% false rejections at a setting of 1% false acceptance) on a per transaction basis. Note: This presumes up to three attempts as a minimum standard error rate.	Biometric Testing (B.1)
BO.6	All TWIC readers should have a finger guide to aid in proper finger placement on the sensor.	Product Review (R.14)

TWIC QTL Portable Physical Access Control Reader Approval Procedures

Requirement ID	Requirement Description	Approval Mechanism
BO.7	All TWIC Readers should be capable of achieving a standard maximum transaction time (defined as the time between presentation of the contactless card to a TWIC reader and completion of the biometric match) of three seconds. Note: This does not include the time required to acquire the TPK either using a magnetic stripe or through download from a PACS.	Applicant Documentation (D.19) Product Review (R.12)
BO.8	For biometrically enabled TWIC readers, the fingerprint sensor should be embedded in the same chassis as the TWIC reader, or if a separate fingerprint sensor module is used, the wiring between the TWIC reader and the biometric unit shall not be exposed.	Product Review (R.13)

Table 13 - Optional Requirements for TWIC Readers supporting Authentication Modes involving biometrics

2 Conformity Assessment Criteria

The following sections outline the criteria (e.g., documentation, artifacts, test results etc.) that are required to be submitted by a vendor to demonstrate conformity with the requirements identified in Section 2.

2.1 Applicant Documentation

Table - 14 outlines the criteria that need to be addressed in the submitted vendor documentation in order to meet the requirement.

Conformity Criteria	**MANDATORY REQUIREMENTS** **D.1 - Mode Configuration** User manual includes the modes that are supported by the Reader and the process to be followed on how to configure the product to operate in each supported mode. Details shall also include the acceptable external triggers that facilitate mode changes. (G.1) (G.21) **D.2 - Canceled Card List Requirements** User manual includes configuration for downloading and using a TWIC Canceled Card List. (P.1) **D.3 - Electrical Requirements** Reader specifications include that the reader's operating voltage is within a range of 8-48 VDC. (G.2) Reader specifications include that the reader's operating amperage doesn't exceed a 2.0 Amperes current requirement. (G.4) Reader Specifications include the provision for reverse voltage protection within the product. (G.5) **D.5 - Clock Configuration** User manual includes details on how to configure the time clock within the product. (P.4) (GO.5) **D.6 - Log Generation Capability** User Manual includes a description of the logging capabilities of the product and the process to be followed to configure and manage this functionality within the product. (G.14) **D.7 - Release Edition** User manual includes details on the release editions and/or test modes that the product supports. (G.23)

D.8 - Contactless Interface
Reader specifications include Applicant claims that the contactless smart card reader component conforms to the ISO/IEC 14443A/B parts 1, 2, 3, and 4 (T=CL protocol) as specified for FIPS 201-1. (G.24)
Reader specifications include Applicant claims that the contactless readers can communicate at speeds of 106kbit/s, 212kbit/s or 424kbit/s with the TWIC Card. (G.26)
OPTIONAL FEATURES

D.9 - Reader Functionality Update
User manual describes the process to be followed for updating reader software/firmware. Updates are permitted only after a successful authentication operation.(GO.1)

D.10 - Test Configuration
User manual includes details on how to configure the product in either test or operational mode. Configuration of this within the reader permits test TWIC cards to be accepted by the product and facilitates testing of the reader and access control system. (GO.2)

D.11 – Wireless connectivity to PACS
User Manual describes the process for configuring session key to be used for communications with the PACS and the available options within the product for authenticating either the reader or the operator to the PACS. (PO.4)

D.12 –Hibernation Mode
User Manual includes configuration for hibernation mode for protection against data loss. (PO.5)

D.13 – Expiration Checking
Reader specifications indicate that the portable reader supports expiration checking (P.6).

D.14 – UL 294 Standard
If portable reader supports connection to a PACS to operate access control devices, reader specifications include Applicant claims that the reader has been tested by an independent laboratory and certified as conformance to the UL 294 Standard for Safety of Access Control System Units, or internationally recognized equivalent (P.5).

D.15 – Communication with an External Access Control System
User Manual describes configuration of the reader for communication with an external access control system to control a door, gate, etc. via a Wiegand or other output format (PO.6).

	CONDITIONAL REQUIREMENTS **D.16 - Lockout Capability** User Manual includes a description of configuration options available within the product for either (i) sending an automated alert and/or (ii) locking out the reader after a configured number of failed biometric matching attempts has been reached. (B.2) **D.17 – Biometric Sensitivity Configuration** User manual describes the process to configure the security sensitivity level for the purposes of 1:1 biometric matching. (BO.4) **D.18 – Liveness Detection** Reader specifications describe the liveness detection capabilities available within the product (BO.1) **D.19 – Transaction Time** Reader specifications describe the time it takes between presentation of the contactless card to a TWIC reader and completion of the biometric match (BO.7)

Table 14 - Applicant Documentation

2.2 Product Review

Table - 15 outlines the set of activities that the QTL Program Management Office (PMO) staff will perform in order to determine conformity with each applicable requirement.

Conformity Criteria	**MANDATORY REQUIREMENTS** **R.1 - Power Supply** Review the product components and determine if a power supply has been provided when operating from a line voltage. (G.3) **R.2 - Reader Design** Examine the reader casing to determine if it possesses any sharp corners or edges that can cause bodily injury. (G.9) Examine the product to determine if there are any external wires, connectors or exposed cabling. (G.10) Examine the product design to check if there are any loose coverings and cowlings (G.11)

R.3 - Visual Indicators
Examine the display and indicators in sunlight to determine its visibility. (G.13)
Examine the readers display to determine its usability (P.2)

R.4 - Product Documentation
Review documentation that accompanies the product to determine completeness of its manuals in terms of installation, operation and maintenance. (G.16)

R.5 - Cryptographic Operations
Cryptographic algorithms have been tested by the NIST Cryptographic Algorithm Validation Program (CAVP) test tool. The AES-128 (ECB mode), SHA-1 and RSA algorithms are supported by the reader's crypto-module. (G.12)

R.6 -Battery Display Configuration
Review the product screen to check whether an indicator for the current battery level is displayed. (P.3)

R.7 - Clock Configuration
Examine the product and configure the time based on the documentation. (P.4)

OPTIONAL FEATURES

R.8 - Product Design
Examine the reader and determine whether the product's edges and corners have at least 1mm radius of curvature (i.e. no sharp corners). (GO.3)

R.9 - Status Display
Examine the reader to determine its capability in displaying its status (e.g. on, ready or out of service) (GO.4)

R.10 – User Input
Examine the readers input to determine its suitability and ease of use (PO.2)

R.11 – Magnetic Stripe Reader Support
Review the product and identify the inclusion of a magnetic stripe reader in the event that the product only has a contactless interface. (PO.3)

R.12 – Transaction Time
Observe and measure the transaction time. (BO.7)

	CONDITIONAL REQUIREMENTS
	R.13 - Product Design - Biometrics Examine the product design to determine whether the fingerprint sensor is embedded in the same chassis as the TWIC reader, or if a separate fingerprint sensor module is used, the wiring between the TWIC reader and the biometric unit is not exposed. (BO.8) **R.14 - Fingerprint Guide** Examine the product to determine the presence and effectiveness of a finger guide to aid the user in proper placement on the sensor. (BO.6)

<center>**Table 15 - Product Review Activities**</center>

2.3 Environmental Testing

Table - 16 outlines the environmental test results that need to be submitted as part of the Applicant documentation in order to meet the applicable requirement

Conformity Criteria:	**CONDITIONAL REQUIREMENTS**
	EN.1 - Vibration Applicants demonstrate product compliance with Method 514.5 from MIL-STD 810F for Vibration. (PH.1) **EN.2 – High Temperature** Applicants demonstrate product compliance with Method 501.4 from MIL-STD 810F for High Temperature (to +70°C/+158°F). (PH.2) **EN.3 – Low Temperature** Applicants demonstrate product compliance with Method 502.4 from MIL-STD 810F for Low Temperature (to -10°C/+14°F). (PH.3) **EN.4 – Humidity** Applicants demonstrate product compliance with Method 507.4 from MIL-STD 810F for Humidity. (PH.4) **EN.5 – Temperature Shock** Applicants demonstrate product compliance with Method 503.4 from MIL-STD 810F for Temperature Shock. (PH.5) **EN.6 – Transit Drop Test** Applicants demonstrate product compliance with Method 516.5, Procedure IV (26 drops at 4 feet) from MIL-STD 810F. (PH.6)

TWIC QTL Portable Physical Access Control Reader Approval Procedures

	EN.7 – NEMA 4 Rating Applicants demonstrate product compliance by providing test results for NEMA 4 rating per NEMA 250:2008 Enclosures for Electrical Equipment (1000 volts maximum). (OUT.1) **EN.8 – Operation in direct Sunlight** Applicants demonstrate the ability of the product to operate in direct sunlight. Examples include the capability of capturing live authentication fingerprints with the mandated Error Rejection Rate (ERR) and the capability to read the instructions displayed. (OUT.2)

Table 16 – Environmental-related test results submission artifacts

2.4 Electrical Testing

Table - 17 outlines the electrical test results that need to be submitted as part of the Applicant documentation in order to meet the applicable requirement

Conformity Criteria:	**MANDATORY REQUIREMENTS** **E.1 - FCC Certification** Applicants demonstrate product compliance with applicable FCC technical requirements in 47 CFR Part 15 and 47 CFR Part 18 and approved in accordance with the FCC equipment authorization procedure. (G.6)

Table 17 - Electrical-related test results submission artifacts

2.5 Safety Testing

Table - 18 outlines the safety related test results that need to be submitted as part of the Applicant documentation in order to meet the applicable requirement.

Conformity Criteria:	**MANDATORY REQUIREMENTS** **S.1 – Safety of Access Control System Units** If the portable TWIC reader supports connection to a PACS to operate access control devices, the product documentation shows evidence of certification in accordance with UL 294 by an OSHA Recognized NRTL with an appropriate scope of recognition. (P.5)

Table 18 - Safety-related test results submission artifacts

2.6 Functional Testing

Table - 19 describes the process used within the TWIC QTL Program to test functionality of the submitted product.

Conformity Criteria:	Conformance with requirements that have an approval mechanism as that of functional testing will be determined based on the test methods provided in the "Portable TWIC Reader Test Procedure" document.

Table 19 - Functional Tests

TWIC QTL Portable Physical Access Control Reader Approval Procedures

2.7 Biometric Testing

Table – 20 outlines the biometric test results that need to be submitted as part of the Applicant documentation in order to meet the applicable requirement

Conformity Criteria:	**CONDITIONAL REQUIREMENTS** **B.1 – Equal Error Rate** Applicants demonstrate product compliance showing how the biometric sub-system on the TWIC Reader provides an equal error rate (EER) of 1% (i.e. 1% false rejections at a setting of 1% false acceptance) on a per transaction basis. (BO.5)

Table 20 – Biometric-related test results submission artifacts

2.8 Reliability Testing

Table - 21 outlines the reliability-related test results that need to be submitted as part of the Applicant documentation in order to meet the applicable requirement.

Conformity Criteria:	**MANDATORY REQUIREMENTS** **RE.1 – Mean Time Between Failure** Applicants demonstrate the capability of their product to have a Mean Time Between Failure (MTBF) of 25,000 hours or greater. (G.15) **CONDITIONAL REQUIREMENTS** **RE.2 – Degradation** Applicants demonstrate the capability of their product to handle 1 million touches without degradation. (B.4)

Table 21 - Reliability-related test results submission artifacts